

A NEW PROOF OF FITZGERALD'S CHARACTERIZATION OF PRIMITIVE POLYNOMIALS

SAMRITH RAM

ABSTRACT. We give a new proof of Fitzgerald's criterion for primitive polynomials over a finite field. Existing proofs essentially use the theory of linear recurrences over finite fields. Here, we give a much shorter and self-contained proof which does not use the theory of linear recurrences.

1. INTRODUCTION

Fitzgerald [1] gave a criterion for distinguishing primitive polynomials among irreducible ones by counting the number of nonzero coefficients in a certain quotient of polynomials. Subsequently, Laohakosol and Pintoptang [2] modified and extended the result of Fitzgerald using similar techniques and appealing to the theory of linear recurrences. Here, we prove Fitzgerald's original result by a more direct approach using elementary properties of the trace map.

2. FITZGERALD'S THEOREM

Theorem 2.1 (Fitzgerald). *Let $p(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree k with $p(1) \neq 0$. Let $m = q^k - 1$ and define $g(x) = (x^m - 1)/(x - 1)p(x)$. Then $p(x)$ is primitive iff $g(x)$ is a polynomial with exactly $(q - 1)q^{k-1} - 1$ nonzero terms.*

Proof. If $p(0) = 0$ then $p(x)$ cannot be primitive. So suppose $p(0) \neq 0$. Then $g(x)$ is a polynomial of degree at most $m - 1$. Let $q(x)$ be the monic reciprocal of $p(x)$ and let $q(x) = (x - \alpha_1) \cdots (x - \alpha_k)$ be the factorization of $q(x)$ in $\mathbb{F}_{q^k}[x]$. Then

$$p(x) = a \prod_{i=1}^k (1 - \alpha_i x)$$

for some $a \in \mathbb{F}_q^*$. We then have the partial fraction decomposition

$$\frac{1}{p(x)} = \frac{1}{a} \sum_{i=1}^k \frac{a_i}{1 - \alpha_i x},$$

2010 *Mathematics Subject Classification.* 11T06, 11T71, 12E05.

Key words and phrases. Irreducible polynomial, Primitive polynomial, Trace.

where $a_i = \alpha_i^{k-1}/q'(\alpha_i)$ for $1 \leq i \leq k$. Expanding each term of the partial fraction formally as a power series and collecting terms, we obtain

$$\frac{1}{p(x)} = \frac{1}{a}(s_{k-1} + s_k x + s_{k+1} x^2 + \cdots),$$

where

$$s_r = \sum_{i=1}^k \frac{\alpha_i^r}{q'(\alpha_i)} = \text{Tr} \left(\frac{\alpha^r}{q'(\alpha)} \right)$$

for each integer r and $\alpha = \alpha_1$. Here, $\text{Tr} : \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q$ is the trace map. Now, we have

$$g(x) = \frac{x^m - 1}{(x-1)p(x)} = \frac{1}{a}(1 + x + \cdots x^{m-1})(s_{k-1} + s_k x + s_{k+1} x^2 + \cdots).$$

Since we already know that $g(x)$ is a polynomial of degree less than m we compute the coefficient of x^t in the above product for $0 \leq t \leq m-1$. This coefficient equals

$$\begin{aligned} \sum_{i=k-1}^{k+t-1} s_i &= \text{Tr} \left(\sum_{i=k-1}^{k+t-1} \frac{\alpha^i}{q'(\alpha)} \right) \\ &= \text{Tr} \left(\frac{\alpha^{k-1}(1 - \alpha^{t+1})}{q'(\alpha)(1 - \alpha)} \right) \\ &= \text{Tr}(\beta) - \text{Tr}(\beta\alpha^{t+1}) \end{aligned}$$

where $\beta = \alpha^{k-1}/q'(\alpha)(1 - \alpha)$. Thus the number of nonzero coefficients in $g(x)$ is equal to the cardinality of

$$\{t : \text{Tr}(\beta) - \text{Tr}(\beta\alpha^{t+1}) \neq 0, 0 \leq t \leq m-1\}.$$

We claim that $\text{Tr}(\beta) \neq 0$. To see this, note that

$$\text{Tr}(\beta) = \sum_{i=1}^k \frac{\alpha_i^{k-1}}{(1 - \alpha_i)q'(\alpha_i)}$$

To compute $\text{Tr}(\beta)$, let y be an indeterminate and consider the Lagrange interpolation polynomial for y^{k-1} at $\alpha_1, \dots, \alpha_k$:

$$\begin{aligned} y^{k-1} &= \sum_{i=1}^k \frac{\alpha_i^{k-1}}{q'(\alpha_i)} \prod_{j \neq i} (y - \alpha_j) \\ &= \sum_{i=1}^k \frac{\alpha_i^{k-1}}{q'(\alpha_i)} \frac{q(y)}{(y - \alpha_i)} \end{aligned}$$

Setting $y = 1$ we find that $\text{Tr}(\beta) = 1/q(1) \neq 0$ (since $p(1) \neq 0$), proving the claim.

Suppose $p(x)$ is primitive. Then $q(x)$ is also primitive and consequently α has multiplicative order $q^k - 1$ in $\mathbb{F}_{q^k}^*$. Therefore, the set $\{\beta\alpha^{t+1} : 0 \leq t \leq m-1\}$ is

precisely $\mathbb{F}_{q^k}^*$. Since the map $\text{Tr} : \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q$ is surjective and all its fibers have the same cardinality, there are precisely q^{k-1} values of t ($0 \leq t \leq m-1$) for which $\text{Tr}(\beta\alpha^{t+1}) = \text{Tr}(\beta)$ (since $\text{Tr}(\beta) \neq 0$). Thus, the number of nonzero coefficients of $g(x)$ in this case is $m - q^{k-1}$.

For the converse, suppose $p(x)$ is not primitive. Then neither is $q(x)$ and hence, the multiplicative order (say e) of α is a proper divisor of $q^k - 1$. In this case, the number (say N) of values of t ($0 \leq t \leq m-1$) for which $\text{Tr}(\beta\alpha^{t+1}) = \text{Tr}(\beta)$ is an integer multiple of $(q^k - 1)/e$. Since $(q^k - 1)/e > 1$ and $(q^k - 1)/e$ is coprime to q^{k-1} , it follows that $N \neq q^{k-1}$. Thus, the number of nonzero coefficients of $g(x)$ cannot be $m - q^{k-1}$. This completes the proof. \square

Remark 2.2. The condition $p(1) \neq 0$ is imposed to rule out the polynomial $p(x) = x - 1$ which is primitive in $\mathbb{F}_2[x]$.

REFERENCES

- [1] R. W. Fitzgerald. A characterization of primitive polynomials over finite fields. *Finite Fields Appl.*, 9(1):117–121, 2003.
- [2] V. Laohakosol and U. Pientoang. A modification of Fitzgerald's characterization of primitive polynomials over a finite field. *Finite Fields Appl.*, 14(1):85–91, 2008.

INSTITUT DE MATHÉMATIQUES DE LUMINY
LUMINY CASE 907
13288 MARSEILLE CEDEX 9
FRANCE

E-mail address: samrith@gmail.com